

United States District Court  
Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

MARC OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.,

Defendants.

Case No. 13-cv-00453-JST

**ORDER DENYING MOTIONS TO  
SEVER WITHOUT PRJEUJICE**

Before the Court are three motions to sever filed by Defendants Twitter, Inc., ECF No. 236, Electronic Arts, Inc. and Chillingo, Ltd., ECF No. 256, and Instagram, Inc., ECF No. 272. Pursuant to Civil Local Rule 7-1(b), the Court hereby finds these motions appropriate for resolution without oral argument, and therefore VACATES the motion hearings scheduled for May 9, 2013. In consideration of the moving papers and related briefing, the Court will deny the motions without prejudice.

**I. ALLEGED FACTS**

This proposed class action was filed on March 12, 2012, in the Western District of Texas, ECF No. 1. The Western District of Texas transferred the action to this Court on January 15, 2013. ECF No. 218.

The operative Second Amended Complaint (“SAC”), ECF No. 103, brings suit against Apple, Inc. and sixteen entities engaged in or owning an interest in entities engaged in the development of Applications (“Apps”) installed on Plaintiffs’ mobile devices, which are manufactured by Apple (“iDevices”) and distributed via Apple’s App Store. The original complaint was filed in response to news reports in February 2012, including a February 15, 2012 article reporting that “the Apps *Foodspotting, Foursquare, Gowalla, Hipster, Instagram, Kik*

1 *Messenger, Path, Twitter, Yelp!*, and (via Defendant Chillingo’s integrated Crystal platform)  
 2 *Angry Birds Classic* and *Cut the Rope* . . . were engaged in surreptitiously transmitting iDevice  
 3 owners’ private, personal address book materials to unapproved recipients.” Id. ¶ 5. The SAC  
 4 alleges that each developer violated federal and state law because “the Apps made by Defendants  
 5 stole their iDevice address books by surreptitiously initiating unnoticeable Internet calls with  
 6 Plaintiffs’ iDevices and transmitting their address books to unauthorized persons.” SAC ¶ 2. The  
 7 SAC defines the proposed class as follows:

8 Plaintiffs and all owners of iDevices who obtained Apps from  
 9 Apple’s App Store that without requesting the iDevice owner’s prior  
 10 consent initiated an unauthorized iDevice call following which the  
 11 owner’s address book materials were copied, uploaded, transmitted,  
 12 and/or disclosed to others and/or remotely stored and/or otherwise  
 remotely used by others, including any of the following Apps: *Angry  
 Birds Classic, Crystal, Cut the Rope, Foursquare, Foodspotting,  
 Gowalla, Hipster, Kik Messenger, Instagram, Path, Twitter, or Yelp!*  
 (the “Class”) and who were damaged thereby.

13 Id. ¶ 46.

14 **A. Allegations Related to Apple**

15 Plaintiffs allege that Apple designed, manufactured, marketed, and sold the iDevices at  
 16 issue. Id. ¶ 84. Those iDevices are Apple’s iPhone, iPad, and iPod Touch. Id. Each iDevice  
 17 comes with certain pre-installed Apps, including the “Contacts” App, which makes it possible for  
 18 users to store their address book contacts on their iDevices. Id. ¶ 89–92. The pre-installed App  
 19 Store App is a central repository for marketing and distributing other Apps designed by Apple or  
 20 third parties. Id. ¶ 93–95. In order to oversee the inclusion of third-party Apps in the App Store,  
 21 Apple created the iOS Developer Program; App developers pay a fee in order to participate in the  
 22 program, and if they charge users for their Apps, Apple charges them thirty percent of App  
 23 revenue. Id. ¶ 98. The only way to obtain a third party App on an iDevice is to use the App  
 24 Store. Id. ¶ 102.

25 Not all Apps submitted by third party developers make it onto the App store. Apple’s iOS  
 26 Developer Program functions as Apple’s “testing, review and legal clearance process.” Id. ¶ 105.  
 27 Through that program, Apple promulgated standards and guidelines by which App developers  
 28 must comply in order to distribute Apps through Apple’s App Store. Id. ¶ 105–08. Plaintiffs

1 allege that Apple “purports to review every app on the App Store based on a set of technical,  
2 content, and design criteria, as well as for reliability, offensive material, malware and privacy  
3 issues.” Id. ¶ 114.

4 Through the program, Apple also provides “editing software, simulators, forums, guides,  
5 design and Approval criteria, code, code resources and libraries, performance enhancing tools,  
6 testing software, and mentoring via access to Apple engineers who ‘provide ... code-level  
7 assistance, helpful guidance, [and] point [the developer] towards the Appropriate technical  
8 documentation to fast-track [his/her] development process.’” Id. ¶ 111. Plaintiffs allege that,  
9 while Apple promises consumers that its operating system protects their privacy, “Apple’s  
10 tutorials and developer sites specifically teach App developers how to code and create Apps that  
11 non-consensually access, manipulate, alter, use and upload the address book maintained on an  
12 owner’s iDevice.” Id. ¶ 112. Nevertheless, Apple’s program guidelines state that “Private data –  
13 like address books – may not be obtained without the users’ consent.” Id. ¶ 118.

14 Plaintiffs allege that Apple has represented to its users that apps such as those discussed in  
15 the SAC would respect users’ privacy: “Apple assures consumers such as Plaintiffs that  
16 Apps from Apple’s ‘curated App Store’ are ‘rigorous[ly] review[ed],’ tested for compliance with  
17 numerous guidelines, and do not ‘suck up consumers’ private information.’ During a September  
18 2008 public presentation, Apple CEO Steve Jobs similarly stated, albeit falsely in retrospect, that  
19 the App Store was not going to distribute malicious apps or apps ‘that invade your privacy’ and  
20 that the App Store supposedly provided Plaintiffs and consumers, ‘freedom from programs that  
21 steal your private data [and] freedom from programs that trash your battery.’” Id. ¶ 127. As part  
22 of those representations, Plaintiffs allege that Apple tells its developers that “the Address Book  
23 database is ultimately owned by the user.” Id. ¶ 129.

24 In contrast, according to the SAC, Apple’s guidelines for designing apps, called iOS  
25 Human Interface Guidelines, encourage developers to steal users’ private data without consent;  
26 the guidelines tell developers, for example, that “[w]hen it makes sense, don’t force people to  
27 give you information you can easily find for yourself, such as their contacts or calendar  
28 information.” Id. ¶ 133. The guidelines also allegedly tell developers: “If possible, avoid

1 requiring users to indicate their agreement to your EULA [End User License Agreement] when  
2 they first start your application.” Id.

3 The SAC alleges that Apple failed in its review process to exclude apps that  
4 surreptitiously steal users’ private address books, and that it has failed to disclose the  
5 vulnerabilities in its operating system that make the theft possible. Id. ¶ 136–37.

### 6 **B. Allegations Related to Twitter**

7 The SAC alleges that Defendant Twitter, Inc. authored the “Twitter” app, “with Apple  
8 providing assistance through the App iOS Developer Program and a digital certificate for the App  
9 to function on iDevices. Following Apple’s review, Apple released and distributed the Twitter  
10 App on the App Store.” Id. ¶ 231. The plaintiffs who installed Twitter on their iDevices allege  
11 that the app presented them with a “Welcome” screen prompting them to “Follow your friends” by  
12 pressing an on-screen button, under which was written in small type: “Scan your contacts for  
13 people you already know on Twitter.” Id. ¶ 232. “Plaintiffs recall no alerts or warnings that their  
14 address books were being taken.” Id. ¶ 234. Plaintiffs allege that Twitter itself has disclosed that  
15 “prior to February 2012, when Twitter App users tapped the [“Follow your friends”] button-bar,  
16 their iDevice silently made a call over the internet and the Twitter App then uploaded all email  
17 addresses and phone numbers from the iDevice owner’s address book to Twitter’s servers, where  
18 Twitter used, stored and planned to keep those materials for up to eighteen months, likely in  
19 unsecure plain text.” Id. ¶ 235. Following reports in February 2012 that the Twitter app  
20 functioned in this manner, Twitter amended its welcome screen to include a warning telling users:  
21 “We will securely upload your contacts to help you find friends and suggest users to follow on  
22 Twitter.” Id. ¶ 237.

### 23 **C. Allegations Related to the Other App Developers**

24 Plaintiffs make substantially similar allegations with respect to moving Defendants  
25 Electronic Arts, Inc. and Chillingo, Ltd. based on their apps “Cut the Rope” and “Angry Birds  
26 Classic,” and Instagram, Inc., based on its app, “Instagram.” Plaintiffs allege that each app  
27 contained a “Find Friends” feature, and that each app uploaded users’ address books without  
28 consent.

**D. Causes of Action**

The SAC contains the following causes of action: invasion of privacy, misappropriation, conversion, trespass to personal property and/or chattels, misappropriation of trade secrets and proprietary information, negligence, violation of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2510, violation of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, violation of the Racketeer Influenced and Corrupt Organizations Act (“RICO”), 18 U.S.C. §§ 1343, 2314 via wire fraud, 18 U.S.C. § 1343, and transportation of stolen property, 18 U.S.C. § 2314, aiding and abetting as to Apple, aiding and abetting as to Defendant Facebook, Inc., and unjust enrichment. The SAC also alleges violation of the Texas statutory prohibition of theft of property, Tex. Penal Code § 31.03, violation of the Theft Liability Act, Tex. Civ. P & Rem. Code §134.001, and violation of the Texas Wiretap Acts, Tex. Code Crim. Proc. Art. 18.20, § 1(3) and Tex. Pen. Code § 16.02(A). Finally, Plaintiffs allege violation of California Penal Code § 502 and violation of the California Wiretap Act, Cal. Penal Code § 630. Plaintiffs also pray for a constructive trust, a declaratory judgment, and injunctive relief.

**II. LEGAL STANDARD**

Federal Rule of Civil Procedure 21 authorizes district courts to, on its own motion or motion by a party, “on just terms,” sever any claim against a party. In evaluating motions to sever pursuant to Rule 21, courts look to Rule 20 for guidance. Bias v. Wells Fargo & Co., No. 12-cv-664-YGR, 2012 WL 2906664, at \*2 (N.D. Cal. July 13, 2012). Under Rule 20(a)(2), permissive joinder of defendants is proper if: “(A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will arise in the action.” Fed. R. Civ. P. 20(a)(2). Even when these requirements are met, courts may employ their broad discretion to sever in order “to protect a party against embarrassment, delay, expense, or other prejudice that arises from including a person against whom the party asserts no claim and who asserts no claim against the party.” Fed. R. Civ. P. 20(b). See United States v. Testa, 548 F.2d 847, 856 (9th Cir. 1977).

Under the joinder rules, “the impulse is toward entertaining the broadest possible scope of

1 action consistent with fairness to the parties; joinder of claims, parties and remedies is strongly  
2 encouraged.” United Mine Workers of Am. v. Gibbs, 383 U.S. 715, 724 (1966). Rule 20’s  
3 authorization of permissive joinder “is to be construed liberally in order to promote trial  
4 convenience and to expedite the final determination of disputes, thereby preventing multiple  
5 lawsuits.” League to Save Lake Tahoe v. Tahoe Reg’l Planning Agency, 558 F.2d 914, 917 (9th  
6 Cir. 1977).

### 7 **III. ANALYSIS**

8 The moving Defendants based their motions on substantially identical arguments. They  
9 characterize this action as an unmanageable suit against over a dozen defendants based on eleven  
10 apps related to each other only by their distribution through Apple’s App Store. Defendants  
11 analogize this case to a personal injury suit against Wal-Mart and the manufacturers of a variety of  
12 sporting goods, such as a fishing rod, a basketball, a camping tent, a yoga mat, and a baseball mat,  
13 “even though the nature of the items is entirely different and the items were manufactured by  
14 different companies, used in different ways at different times, and involved injuries to different  
15 people.” ECF No. 278 p. 5.

16 In contrast, Plaintiffs characterize their claims against Apple and the app developer  
17 Defendants as inseparable because “[I]like conjoined twins, they are tied at the hip in this matter.”  
18 ECF No. 298. Plaintiffs argue that each app developer and Apple are joint tortfeasors because  
19 they “assisted, collaborated, and conspired with one another and mutually benefited from their  
20 wrongful, harmful acts.” Plaintiffs point to their allegations that: Plaintiffs obtained each app  
21 from Apple; Apple approved and released each app over the App Store; each app was created  
22 using Apple-supplied tools, code, components, and certificates; the app developers were bound by  
23 Apple’s app design guidelines; and each app collected Plaintiffs’ address books from Plaintiffs’  
24 iDevices in violation of Apple’s standards and agreements. In Plaintiffs’ view, although the app  
25 developers are liable independent of one another, each one is jointly liable with Apple, and that  
26 relationship justifies joinder. Plaintiffs also point to the transfer order issued by the Western  
27 District of Texas, based in part on the fact that similar class actions are pending in this district, in  
28 which the transferee court observed: “To try this case separately virtually guarantees a waste of

1 judicial resources, and risks inconsistent rulings.” ECF No. 217 p. 7.

2 None of the cases cited by the parties are factually analogous to the instant one.  
3 Defendants point to a variety of cases where the plaintiffs did not allege joint and several liability.  
4 For example, in EIT Holdings LLC v. Yelp!, Inc., 10-cv-05623-WHA, 2011 WL 2192820, at \*1  
5 (N.D. Cal. May 12, 2011), the plaintiff named nine defendants alleged to have infringed on the  
6 same two patents. They were not “alleged to have acted in concert to infringe plaintiff’s asserted  
7 patent.” Similarly, in San Francisco Tech., Inc. v. Adobe Sys. Inc., 10-cv-01652-RS, 2010 WL  
8 1640397, at \*1 (N.D. Cal. Apr. 19, 2010), the plaintiff sued fourteen unrelated companies for  
9 allegedly marking products with expired patent numbers, in violation of 35 U.S.C. § 292. The  
10 plaintiff did not allege any connection among the defendants. Defendants’ reliance on Bias v.  
11 Wells Fargo & Co., No. 12-cv-664-YGR, 2012 WL 2906664, at \*2–3 (N.D. Cal. July 13, 2012), is  
12 also misplaced. Id. (“There are no allegations of any conspiracy, concerted action, or RICO  
13 enterprise as between the Defendants groups.”).

14 Defendants also cite several decisions finding misjoinder where copyright holders have  
15 sued dozens of defendants for downloading copyrighted works independently. See, e.g., AF  
16 Holdings LLC v. Does 1-97, No. 11-cv-03067-CW, 2011 WL 2912909, at \*2–3 (N.D. Cal. July  
17 20, 2011) (“Attempts to join numerous defendants in a single action for copyright infringement  
18 over P2P networks historically have failed.”). Those decisions hold only that, absent an allegation  
19 that any of the downloading defendants downloaded from one another, there cannot be a common  
20 transaction or occurrence.

21 Plaintiffs do not point to any analogous decisions either, but their allegations, evaluated  
22 now at the pleading stage, make clear that they allege joint and several liability against Apple and  
23 each app developer arising out of a common transaction or occurrence: Apple’s role in marketing,  
24 testing, reviewing, and distributing the subject apps. That allegation satisfies the first requirement  
25 of Rule 20(a)(2). See Hubbard v. Hougland, No. 09-cv-0939, 2010 WL 1416691, at \*7 (E.D. Cal.  
26 Apr. 5, 2010) (“The ‘same transaction’ requirement of Rule 20 refers to ‘similarity in the factual  
27 background of a claim; claims that arise out of a systematic pattern of events’ and have a ‘very  
28 definite logical relationship.’” (quoting Bautista v. Los Angeles Cnty., 216 F.3d 837, 842–843 (9th

United States District Court  
Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

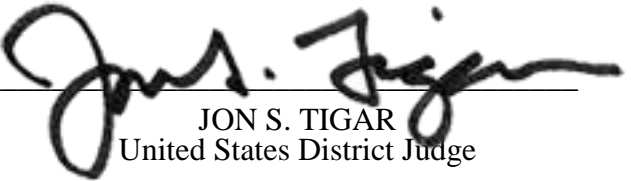
Cir.2000)).

Plaintiffs' case against each app developer will also necessarily involve common questions of fact and law with respect to Apple, satisfying the second requirement for permissive joinder. The Court finds that the requirements of Rule 20(a)(2) have been met, and that the moving Defendants have failed to make a showing of prejudice. The motions to sever are denied without prejudice. Defendants may renew their motions at a later date if subsequent developments in the case make severance more appropriate.

For the foregoing reasons, Defendants Twitter, Inc., Electronic Arts, Inc., Chillingo, Ltd., and Instagram, Inc.'s motions to sever are hereby DENIED without prejudice.

**IT IS SO ORDERED.**

Dated: May 6, 2013

  
\_\_\_\_\_  
JON S. TIGAR  
United States District Judge